



State of Iowa Enterprise Printer & Copier Guidance

July 22, 2010

Printers, copiers and related devices are capable of storing large volumes of information. Recent news coverage has highlighted the fact that confidential information can be recovered from printers, copiers and similar devices after they are sent to surplus or returned to the vendor at the end of their lease.

Because of the risk of a data breach associated with the use of printers, copiers, scanners and faxes agencies should review how these devices are disposed of. Current Enterprise Security Standards require that:

Devices and media containing confidential data shall be erased with a DoD approved method prior to disposal.

Agencies should review the following for printers, copiers, scanners, and faxes:

- **Inventory:** Review the types of printers\copiers\scanner\faxes used in the agency and their physical location.
- **Settings:** Configure agency printers\copiers\scanner\faxes securely.
- **New Devices:** Purchase\lease devices with disk encryption and immediate data overwriting capability.
- **Disposal:** Send all printers\copiers\scanner\faxes to IT staff so that the hard drives may be removed and wiped before surplus\return to vendor.
- **Public Devices:** Do not use public printers\copiers\scanner\faxes for documents containing confidential state information.

Agencies with questions regarding the security of printers, copiers, scanners and faxes may contact the DAS-Information Security Office at 515-281-4820.

Resources:

Xerox <http://www.xerox.com/information-security/product/enus.html>

Ricoh <http://www.oit.uci.edu/security/RicohCommonSecurityFeaturesGuide.pdf>

Cannon <http://www.usa.canon.com/html/security/index.html>

hp <http://h71028.www7.hp.com/enterprise/cache/617575-0-0-225-121.html>

Toshiba <http://www.copiers.toshiba.com/usa/security/device-security/index.html>